UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,223	05/22/2000	Nicholas Anthony John Peach	140/238 [UK999-051]	2229

30678   7590   01/07/2005

CONNOLLY BOVE LODGE & HUTZ LLP
SUITE 800
1990 M STREET NW
WASHINGTON, DC 20036-3425

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- Th MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _29 July 2004_.

2a) ☒ This action is **FINAL.**   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-21_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-21_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed July 29, 2004 have been fully considered but they are
not persuasive.

It is argued by the applicant that the teachings of Fischer fail to disclose of "a
validating signature generated from rules and the body according to a first key
belonging to a validating party, and a sealing signature generated from the header
package and the sealed packages according to a second key belonging to the sealing
party." The examiner respectfully disagrees. The teachings of Fischer are directed
towards digitally signing documents for verification and for presenting a set of hashed
rules to indicate if the document was altered in any manner, see column 4, lines 62-66
and column 8, lines 1-41 of Fischer.

It is additionally argued by the applicant that the combined teachings of Hall,
Fischer, and Ginter fail to disclose of "requiring rules to be embedded in a header
package and identify the various packages and signatures to produce a contract." The
examiner respectfully disagrees for the teachings of Hall are relied upon for this feature.
Hall demonstrates of the usage of a header package, please see Figure 10B. The
teachings of Hall are directed towards digital rights management, which are rules, or a
contract, governing the usage of protected resources (see column 1, lines 55-65). The
rules, contained within the header of the secure container, limit how the protected
software is to be used and enforces the usage conditions (column 20, lines 30-35). The

teachings of Fischer and Ginter are not relied upon for showing of "requiring rules to be

embedded in a header package." Fischer is relied upon for the disclosure of signatures

to produce a contract, please refer to column 8, lines 1-21 of Fischer.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-2,4-11,13-19, and 21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Hall et al (U.S. Patent 6,138,119 and Hall hereafter) in view of

Fischer (U.S. Patent 5,214,702).

In regards to claim 1, Hall teaches a digital file (i.e. container) (see col. 1, line 40)

forming a contract (i.e. agreement) (col. 1, line 61) comprising:

a header package (figure 10B) having rules (figure 5, element 316) defining

sealed packages produced by a sealing party; and

a body (i.e. associated object) (col. 20, lines 5-13, and figure 5, element 102)

containing at least a portion of the content of the contract.

Hall does not teach a validating signature generated from the rules and the body

according to a first key belonging to a validating party; and a sealing signature

generated from the header package and the sealed packages according to a second

key belonging to said sealing party.

Fischer teaches a validating signature generated from the rules and the body according to a first key belonging to a validating party; and a sealing signature generated from the header package and the sealed packages according to a second key belonging to said sealing party.

That is, Fischer teaches a methodology by which multiple objects such as, for example, a cover letter, and associated enclosed letter, an associate graphics file, etc., may be signed together in such a way that each object is individually verifiable and while also indicating the relationship of each object to the whole group. An aggregation of data related to all of these objects (possibly the HASH of each of these objects together with control information) is gathered into an ordered list. This ordered list is then viewed as an object and is signed or the hash of the list is signed. This list shows that the signer individually recognized the associated objects as well as their context in the group. Thus, each element of this ordered list is processed by a hashing algorithm (to generate a more compact version thereof) which results in a list of presignature hash values. The presignature hash list is then run through a decrypt (signature) cycle to result in the signer's signature, hereinafter referred to as seal, which becomes part of the signature packet as will be described in detail below. (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include a validating signature generated from the rules and the body according to a first key belonging to a validating party; and a sealing signature generated from the header package and the sealed packages according to a second key belonging to said sealing

party with the motivation to individually verify each object while also indicating the

relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 2, Hall teaches wherein said header package further

comprises a unique header identifying a type (i.e. environment) of said sealed package

(col. 20, lines 1-4).

Hall does not teach that said validating signature is generated from said rules,

said body and said header.

Fischer teaches that said validating signature is generated from said rules, said

body and said header (i.e. an aggregation of data related to all of these objects

(possibly the HASH of each of these objects together with control information) is

gathered into an ordered list. This ordered list is then viewed as an object and is signed

or the hash of the list is signed) (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time

of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to

include that said validating signature is generated from said rules, said body and said

header with the motivation to individually verify each object while also indicating the

relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 4, Hall teaches wherein said rules define one or more

unsealed packages to be included in said sealed package, said body comprises a

HTML file and one of the unsealed packages defined in the rules contains data for a

field the HTML file (i.e. descriptive data structures 200 can be used to define the format

and/or other characteristics associated with a wide variety of different types of digital

information) (col. 11, lines 35-40). The office infers that "a wide variety of different types

of digital information" includes an HTML file.

In regards to claim 5, Hall teaches wherein said rules comprise a URL (col. 14,

line 50) corresponding to the location for which each sealed package to be included in

the contract can be obtained.

In regards to claim 6, Hall teaches wherein said URL is a CGI script (i.e. software

program) for commanding (i.e. driving) a remote server (i.e. automated packaging

application) to generate said sealed package (see col. 7, lines 61-64).

In regards to claim 7, Hall teaches wherein said URL (col. 14, line 50) identifies

the location (col. 14, lines 34-39) of said sealed package.

In regards to claim 8, Hall teaches a contract management apparatus (figure 8)

for validating a digital file (i.e. container) (see col. 1, line 40) constituting a contract (i.e.

agreement) (col. 1, line 61), said digital file having a header package (figure 10B) which

includes rules (figure 5, element 316) defining sealed packages, a body (i.e. associated

object) (col. 20, lines 5-13, and figure 5, element 102) containing at least a portion of the

contract, and a validating signature (figure 10B, elements 812B and 819), comprising:

means for reading (i.e. parsing) (figure 10A, element 852, and col. 20, lines 14-22) said rules and for identifying a validating party and a sealing party (i.e. trusted certifying authority) (col. 19, lines 42-67) which created a sealed file of said contract;

first means for obtaining a first key belonging to said validating party cooperable with said validating signature generated from said rules and body to validate said header package (i.e. a target environment would need to acquire a corresponding cryptographic key (e.g. a public key of a public key/private key pair) using trusted techniques (e.g. delivery in a certificate signed by a trusted certifying authority) in order to evaluate such a source message) (col. 19, lines 55-60);

means for iteratively validating any sealed packages contained in contract using said second key and sealing signature (col. 19, lines 28-41).

Hall does not teach second means for obtaining a second key belonging to said sealing party cooperable with said sealing signature to validate said contract.

Fischer teaches second means for obtaining a second key belonging to said sealing party cooperable with said sealing signature to validate said contract (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include second means for obtaining a second key belonging to said sealing party cooperable with said sealing signature to validate said contract with the motivation to individually verify each object while also indicating the relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 9, Hall teaches wherein said iterative validating means returns any data stored in said sealed packages (col. 20, lines 14-49).

In regards to claim 10, Hall teaches further comprising means for displaying said body contents and said returned data (col. 20, lines 14-49). The office infers that "any other application" pertaining to object 830 also includes the display of its body contents.

In regard to claim 11, Hall teaches a contract management apparatus (figure 8) for generating a digital file (i.e. container) (see col. 1, line 40) constituting a contract (i.e. agreement) (col. 1, line 61) comprising:

means for obtaining a header package (figure 10B) for said contract;

means for reading (i.e. parsing) rules defining sealed data packages (col. 20, 14-49),and for identifying a sealing party and any sealed packages to be included in said contract (col.19, lines 20-27);

means for obtaining said identified sealed packages (col. 20, lines 11-13);

means for generating a sealing signature from said Header package and any of said sealed packages according to a first key belonging to said sealing party (col. 19, lines 20-67); and

means for assembling (i.e. packaging) said header package, sealed packages and said sealing signature into said digital file constituting a contract (col. 20, lines 5-13).

In regards to claim 13, Hall teaches one of a smartcard, a personal digital assistant, a personal computer, a terminal or an embedded system (i.e. electronic appliance) (col. 12, lines 34-52).

In regards to claim 14, Hall teaches a computer product for storing instructions which are executed by a computer to validate a digital file (i.e. container) (see col. 1, line 40) having a leader package (figure 10B) which includes rules (figure 5, element 316) defining sealed packages, a body (i.e. associated object) (col. 20, lines 5-13, and figure 5, element 102) containing at least a portion of a contract (i.e. agreement) (col. 1, line 61) and a validating signature (figure 10B, elements 812B and 819) comprising:

reading said digital file and identifying a validating party and a sealing party (i.e. trusted certifying authority) (col. 19, lines 42-67) which created a sealed package of said contract;

deriving a first key belonging to a validating party (col.19, lines 55-67);

validating said header package using said first key and said validating signature (col. 19, lines 42-48).

Hall does not teach deriving a second key belonging to said sealing party;

deriving a sealing signature from said header package; and validating said digital file using said second key and said sealing signature.

Fischer teaches deriving a second key belonging to said sealing party; deriving a sealing signature from said header package; and validating said digital file using said second key and said sealing signature. (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include a validating signature generated from the rules and the body according to a first key belonging to a validating party; and a sealing signature generated from the header package and the sealed packages according to a second key belonging to said sealing party with the motivation to individually verify each object while also indicating the relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 15, Hall does not teach instructions for deriving said sealing signature from a unique number contained in said header package.

Fischer teaches instructions for deriving said sealing signature from a unique number contained in said header package (i.e. an aggregation of data related to all of these objects (possibly the HASH of each of these objects together with control information) is gathered into an ordered list. This ordered list is then viewed as an object and is signed or the hash of the list is signed) (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include that said validating signature is generated from said rules, said body and said

header with the motivation to individually verify each object while also indicating the relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 16, Hall teaches a computer product (i.e. descriptive data structure) (col. 11, lines 24-25) storing instructions for execution on a computer to perform a process to validate a digital file (i.e. container) (see col. 1, line 40) constituting a contract (i.e. agreement) (col. 1, line 61) comprising the steps of:

unzipping a header package in said digital file and reading rules contained in said header package (i.e. parsing it to locate the target data block, col. 20, lines 18-27);

determining from said rules keys to validate said header package constituting said contract (col. 20, lines 36-40); and

validating each sealed package in said digital file using said keys (col. 19, lines 20-27).

Hall does not teach determining from said rules keys to validate a sealed package of said digital file.

Fischer teaches determining from said rules keys to validate a sealed package of said digital file (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include determining from said rules keys to validate a sealed package of said digital file with the motivation to individually verify each object while also indicating the relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 17, Hall teaches further comprising instructions for performing tile additional steps of obtaining said keys from a network server identified by said rules (i.e. publishing the certificate on a public network, etc) (col. 19, line 35-41).

In regards to claim 18, Hall teaches a computer product (i.e. descriptive data structure) (col. 11, lines 24-25) for storing instructions for a computer to execute the process comprising the steps of:

storing rules (i.e. metadata, figure 7, element 264) to describe a data package

creating from said rules a data package containing a digital data file (figure 2B):

merging (i.e. packaging) said rules and said data package into a merged file (col. 20, lines 5-11);

creating a package validity signature from said merged file to prevent unauthorized use of said digital file (figure 10B, elements 812B and 819); and

generating a unique number identifying said digital file (figure 10B, element 813)

merging (i.e. packaging) (col. 12, lines 23-27) said package validity signature, said merged file and said unique number;

Hall does not teach creating a sealing signature from said merged files; and

sealing said merged files with said sealing signature to produce a sealed package.

Fischer teaches creating a sealing signature from said merged files; and sealing said merged files with said sealing signature to produce a sealed package (col. 8, lines 1-21).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer to include creating a sealing signature from said merged files; and sealing said merged files with said sealing signature to produce a sealed package with the motivation to individually verify each object while also indicating the relationship of each object to the whole group (Fischer, see column 8, lines 5-7).

In regards to claim 19, Hall teaches wherein said rules comprises a plurality of elements (figure 10B) which point to a location on said computer containing a required package (i.e. other descriptive data structures) (col.11, line 55; col. 14, lines 34-39).

In regards to claim 21, Hall teaches wherein said merged files are compressed (i.e. packaged) as a single file (col. 20, lines 5-7).

4.   Claims 3 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over over Hall in view of Fischer in view of Ginter (U.S. Patent 6,185,683 and Ginter hereinafter).

In regards to claim 3, Hall does not teach wherein said sealed package comprises a unique number generated by said sealing party and said sealing signature is generated from said header package, any of said sealed packages and said unique number.

Fischer teaches that the sealing signature is generated from said header package, any of said sealed packages and said unique number (i.e. an aggregation of data related to all of these objects (possibly the HASH of each of these objects together with control information) is gathered into an ordered list. This ordered list is then viewed as an object and is signed or the hash of the list is signed) (col. 8, lines 1-21). Ginter teaches that the sealed package comprises a unique number generated by said sealing party (i.e. the text and/or graphics contents of item 4054 can be transformed into a compact value using a special cryptographic function called a "one-way hash" 4212. The resulting number may be "concatenated" (i.e., put end to end) with other information such as, for example, a time value and a certificate value or number obtained from a "digital certificate" 4214. The time value may be obtained from a real time clock 528 incorporated in secure processing unit (SPU) 500 shown in FIG. 9. The resulting string of digital information may then be encrypted with the private cryptographic key of sender 4052, the contracting party 4070 and/or system 4050. The resulting digital signature value 4216 may be used to encode some or all of the seal 4200's pattern) (col. 28, lines 50-63).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Fischer and Ginter to include wherein said sealed package comprises a unique number generated by said sealing party and said sealing signature is generated from said header package, any of said sealed packages and said unique number with the motivation to establish the authenticity of the document (for example, preventing a signatory from repudiating it

and to allowing it to be admitted as evidence in a court of law). (Ginter, see column 22, lines 11-15).

In regards to claim 20, Hall does not teach wherein said rules define a sealing signature for said sealed package.

Ginter teaches wherein said rules define a sealing signature for said sealed package (i.e. Appliance 600B may deliver the digital copy of item 4054 within a container 302 and/or may protect the item with seals, electronic fingerprints, watermarks and/or other visible and/or hidden markings to provide a "virtual container" or some of the security or other characteristics of a container) (col. 18, lines 50-54).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Hall with the teachings of Ginter to include wherein said rules define a sealing signature for said sealed package with the motivation to establish the authenticity of the document (for example, preventing a signatory from repudiating it and to allowing it to be admitted as evidence in a court of law) (Ginter, see column 22, lines 11-15).

5.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hall in view of Ginter in further of Tedesco et al (U.S. Patent 6,282,523 and Tedesco hereinafter).

In regards to claim 12, Hall teaches a contract management apparatus comprising:

means for accepting and securely storing data files constituting contracts in an

encrypted package database (i.e. a mass storage device or other memory) (col. 11,

lines 65-66);

a navigator tool adapted to allow a user access to said stored data files

constituting said contracts (figure 3, element 306); and

means, responsive to a request for an encrypted package from said data base,

for transmitting said package to an external entity (col. 11, lines 32-34)

Hall does not teach means for backing-up said package database; means for

informing users of data files having expiring contracts in said data base; and means for

deleting contracts from said data base.

Ginter teaches means for backing-up said package database (figures 39 and 40);

and means for deleting contracts from said data base (i.e. the user options associated

with a contract offer (which are used to create electronic controls associated with the

electronic transaction) might relate to a suggested addition, modification, deletion, etc.

to an existing item) (col. 35, lines 44-47).

Therefore it would have been obvious to one of ordinary skill in the art at the time

of Applicant's invention to modify the teaching of Hall with the teachings of Ginter to

include means for backing-up said package database; and means for deleting contracts

from said data base with the motivation to provide enhanced and automated

functionality, features and other advantages (Ginter, see column 9, lines 13-14).

The combination of Hall and Ginter, however, does not teach means for

informing users of data files having expiring contracts in said data base.

Tedesco teaches means for informing users of data files (i.e checks) having

expiring contracts in said data base (col. 13, lines 10-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time

of Applicant's invention to modify the teaching of Hall and Ginter with the teachings of

Tedesco to include means for informing users of data files (i.e checks) having expiring

contracts in said data base with the motivation to reduce the hesitancy to receive

checks (Tedesco, see column 3, lines 23-24).

Conclusion

6.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christopher A. Revak whose telephone number is 571-

272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

January 3, 2005

EMMANUEL L. MOISE
PRIMARY EXAMINER